+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 16/05/2025

Sign up

Forcepoint Data Security Cloud training

3 days (21 hours)

Presentation

Our Forcepoint Data Security Cloud training course will enable you to master modern data protection techniques in a cloud environment thanks to an intelligent, scalable platform. You'll learn how deploy effective security strategies, monitor risky activities and ensure regulatory compliance.

Our training program covers all the essential basics, right through to advanced features, so you'll be able to classify, protect and monitor your sensitive data in a hybrid or full cloud environment, with centralized management.

At the end of this course, you'll know how to create multi-channel DLP rules, set up real-time adaptive monitoring and respond effectively to incidents.

As with all our training courses, this one uses the latest version of Forcepoint 9.0.

Objectives

- Understand the fundamental concepts of data security in the cloud .
- Master the use of the Forcepoint console to apply unified security policies.
- Create policies adapted to hybrid environments.
- Using Forcepoint effectively in modern environments.
- Structuring and documenting a data security framework.

Target audience

- Cybersecurity analysts
- IT project managers
- DPO

Prerequisites

- A solid grounding in HTML and CSS
- Notions of responsive design
- Knowledge of JavaScript

Program of our Forcepoint Data Security Cloud training course

Introduction to Forcepoint

- Forcepoint presentation and solution
- Overview of data threats
- Forcepoint Data Security Cloud architecture
- Component overview
  - AI Mesh
  - DDR
  - DSPM
- Typical use cases

Forcepoint platform management

- Logging in and navigating the cloud portal
- Administration interface
- User creation and access management
- Integration with LADP/AD directory
- Data Inventory & Discovery
- Connector configuration
  - Web
  - E-mail
  - Cloud Apps

Security policy and data classification

- Automatic and manual classification
- Creating classification models with AI Mesh
- Multi-channel DLP rules
  - Cloud
  - Web
  - Endpoint
- RGPD, HIPAA

Supervision, alerts and incident response

- Real-time monitoring with DDR

- Risk-Adaptive Protection
- Security incident management
- Workflow creation
- Reports and dashboards
- Audit & traceability of events

Deployment, compliance and best practices

- Deployment
  - multi-site
  - hybrid
- Integration with SIEM or SOAR
- Configuration backup & restore
- Preparing for the compliance audit
- Best practice in regulated environments

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives with regard to the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.